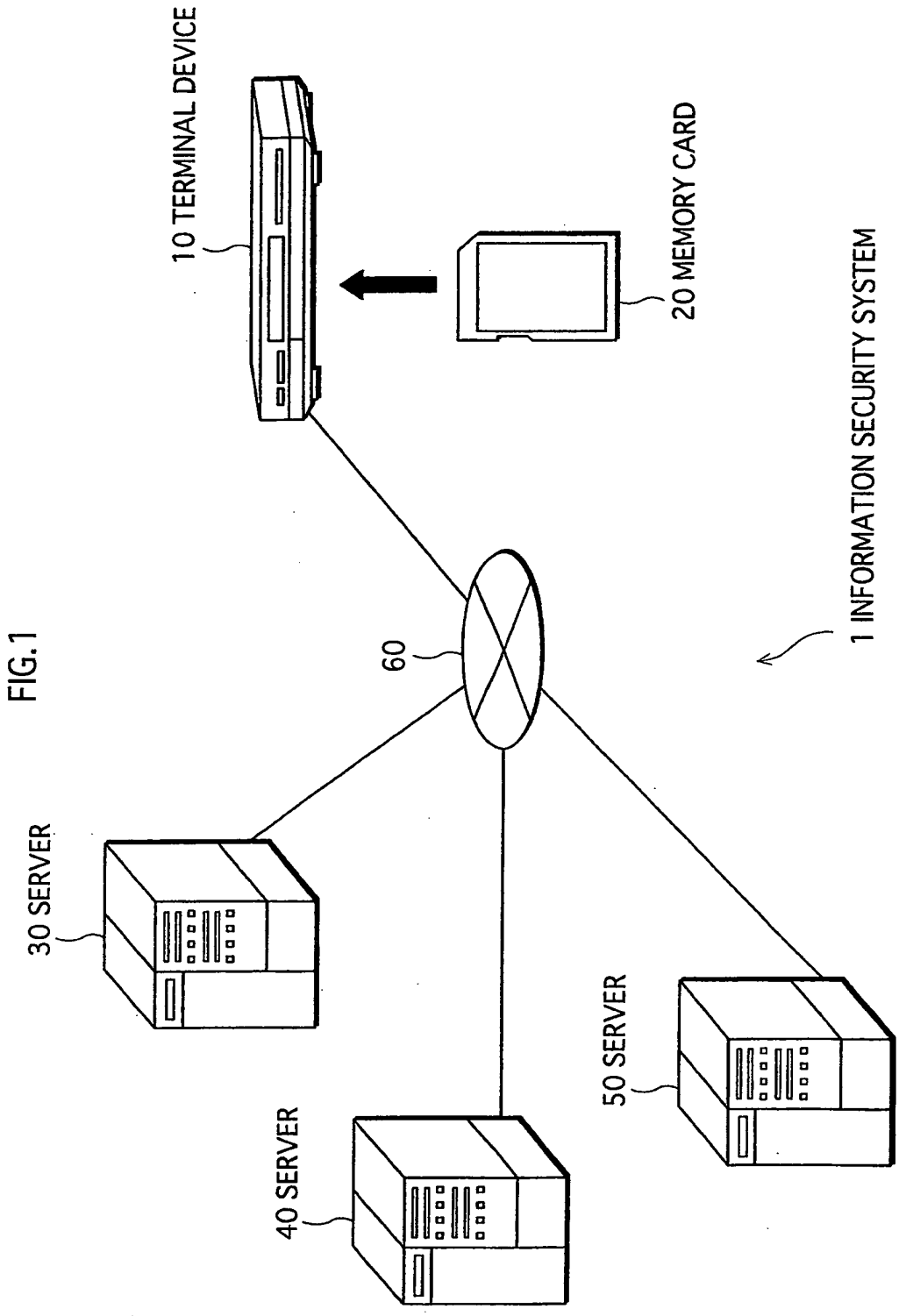

10 TERMINAL DEVICE
20 MEMORY CARD
1 INFORMATION SECURITY SYSTEM
60
30 SERVER
40 SERVER
50 SERVER

FIG.1

FIG.2

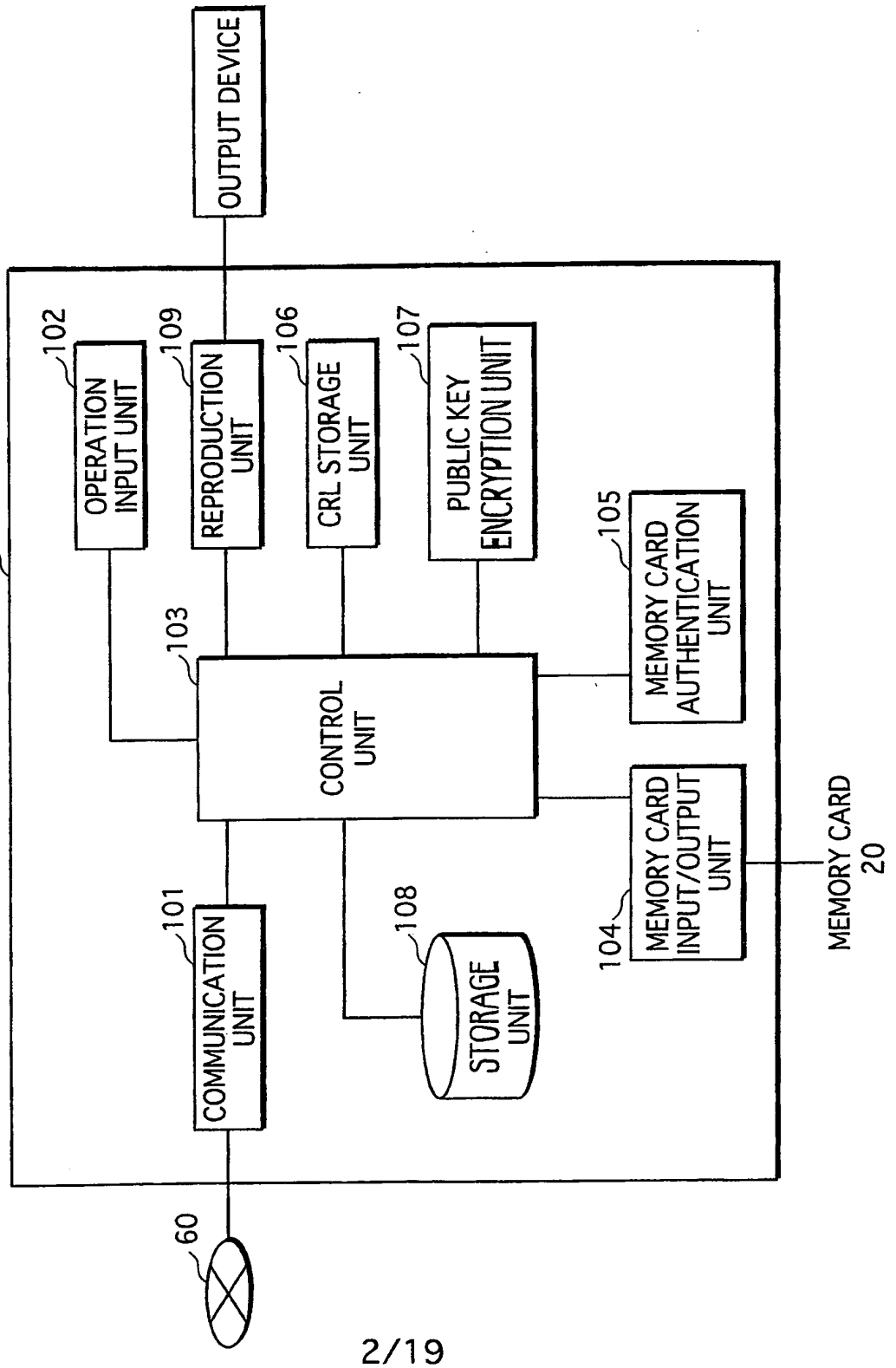

OUTPUT DEVICE
10 TERMINAL DEVICE
102
OPERATION INPUT UNIT
109
REPRODUCTION UNIT
106
CRL STORAGE UNIT
107
PUBLIC KEY ENCRYPTION UNIT
105
MEMORY CARD AUTHENTICATION UNIT
103
CONTROL UNIT
MEMORY CARD INPUT/OUTPUT UNIT
104
MEMORY CARD 20
101
COMMUNICATION UNIT
108
STORAGE UNIT
60

FIG.3A

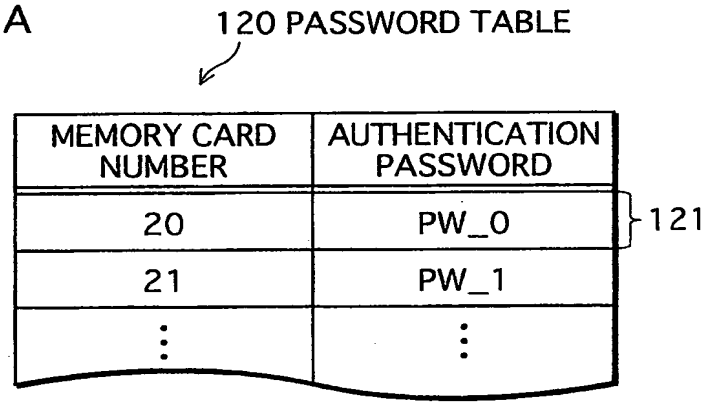

120 PASSWORD TABLE
MEMORY CARD NUMBER
AUTHENTICATION PASSWORD
20
PW_0
121
21
PW_1

FIG.3B

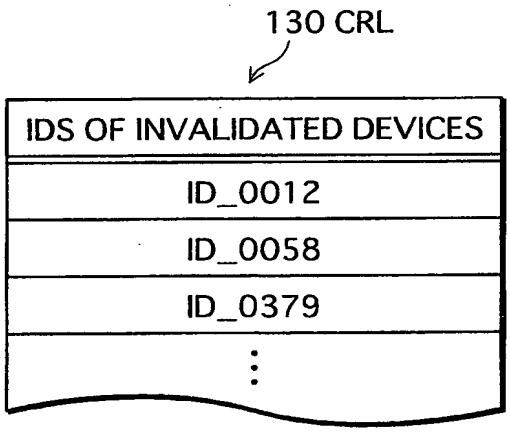

130 CRL
IDS OF INVALIDATED DEVICES
ID_0012
ID_0058
ID_0379

FIG.4

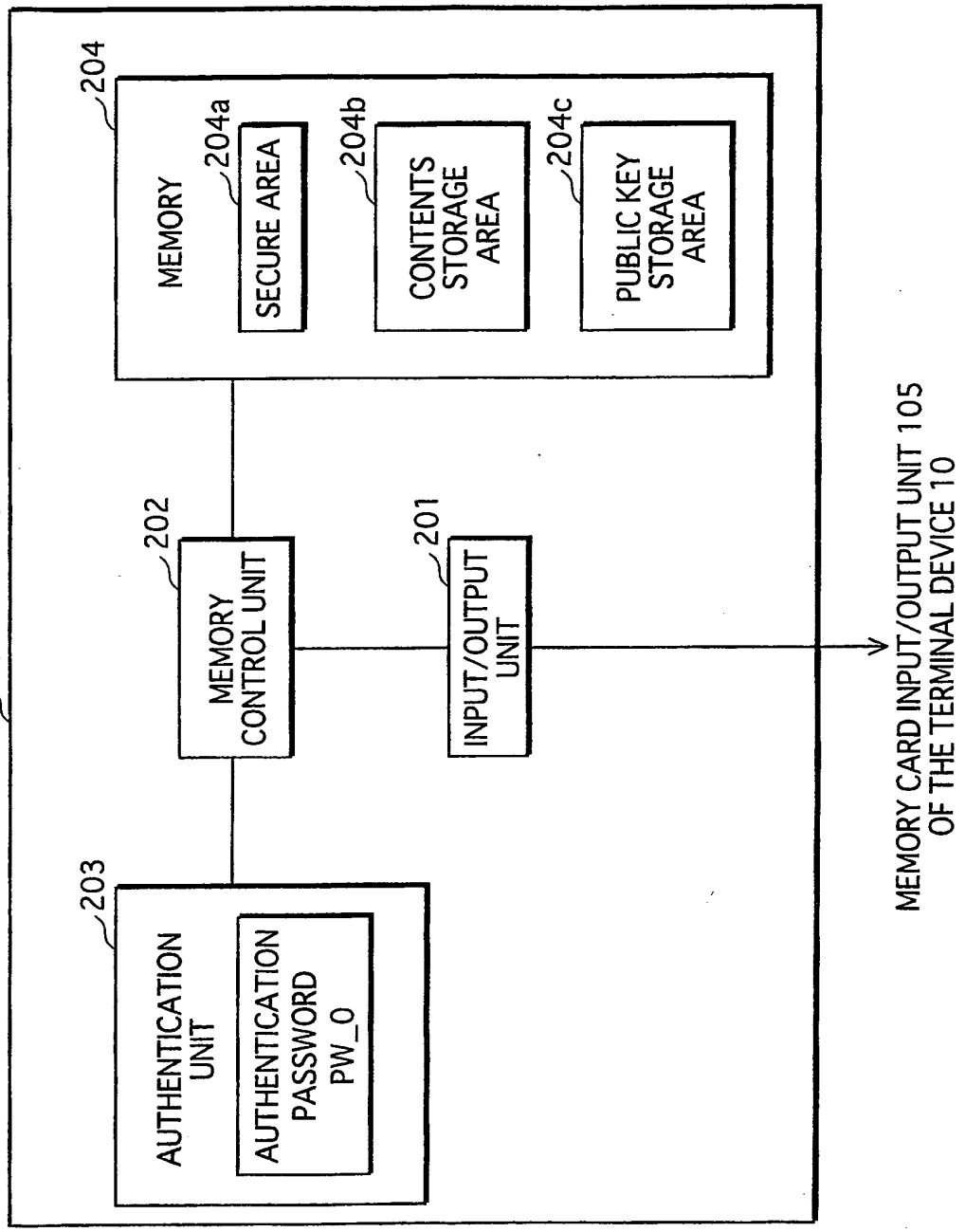

20 MEMORY CARD
204
MEMORY
204a
SECURE AREA
204b
CONTENTS STORAGE AREA
204c
PUBLIC KEY STORAGE AREA
202
MEMORY CONTROL UNIT
201
INPUT/OUTPUT UNIT
203
AUTHENTICATION UNIT
AUTHENTICATION PASSWORD PW_0
MEMORY CARD INPUT/OUTPUT UNIT 105 OF THE TERMINAL DEVICE 10

FIG.5

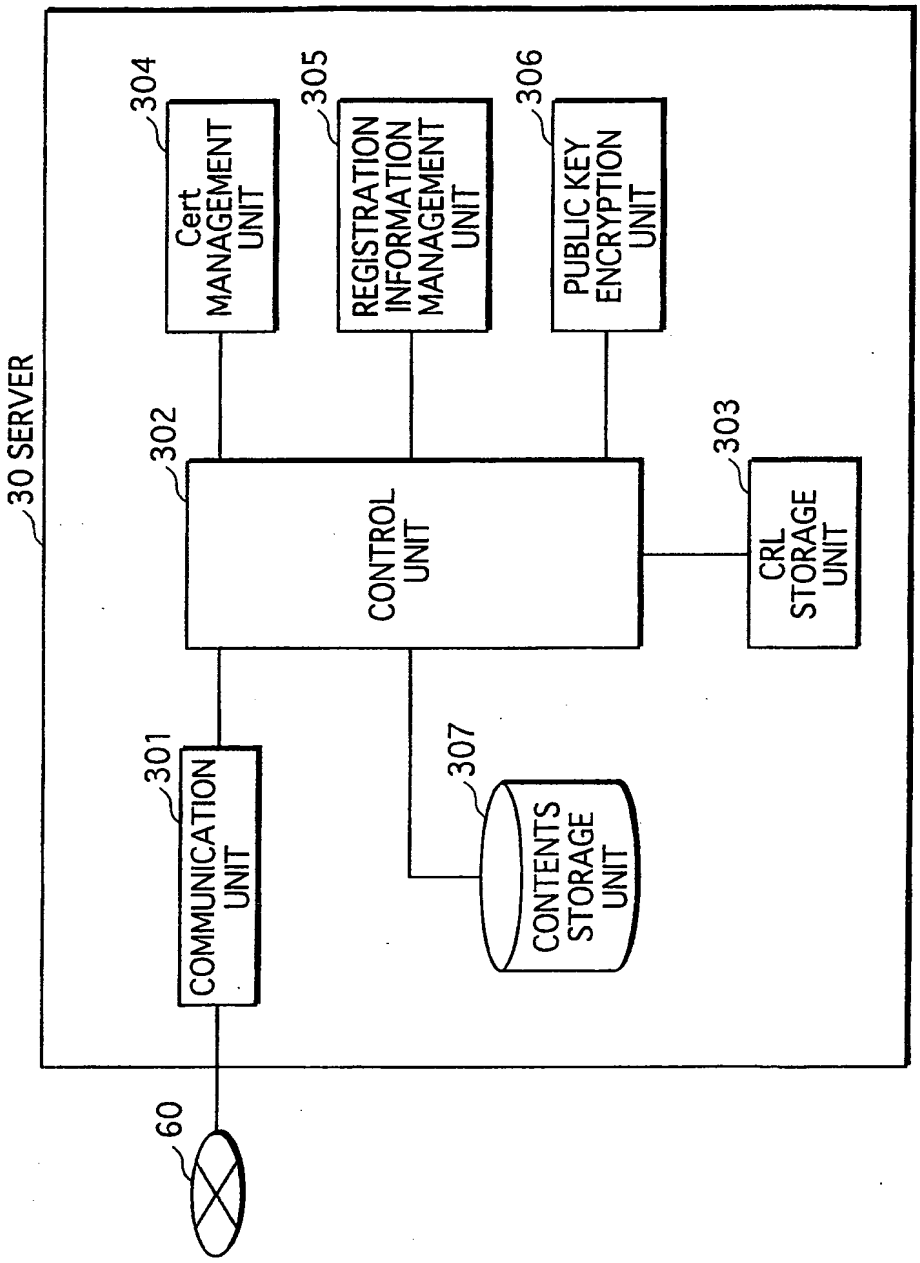

30 SERVER
304
Cert MANAGEMENT UNIT
305
REGISTRATION INFORMATION MANAGEMENT UNIT
306
PUBLIC KEY ENCRYPTION UNIT
302
CONTROL UNIT
303
CRL STORAGE UNIT
301
COMMUNICATION UNIT
307
CONTENTS STORAGE UNIT
60

FIG.6

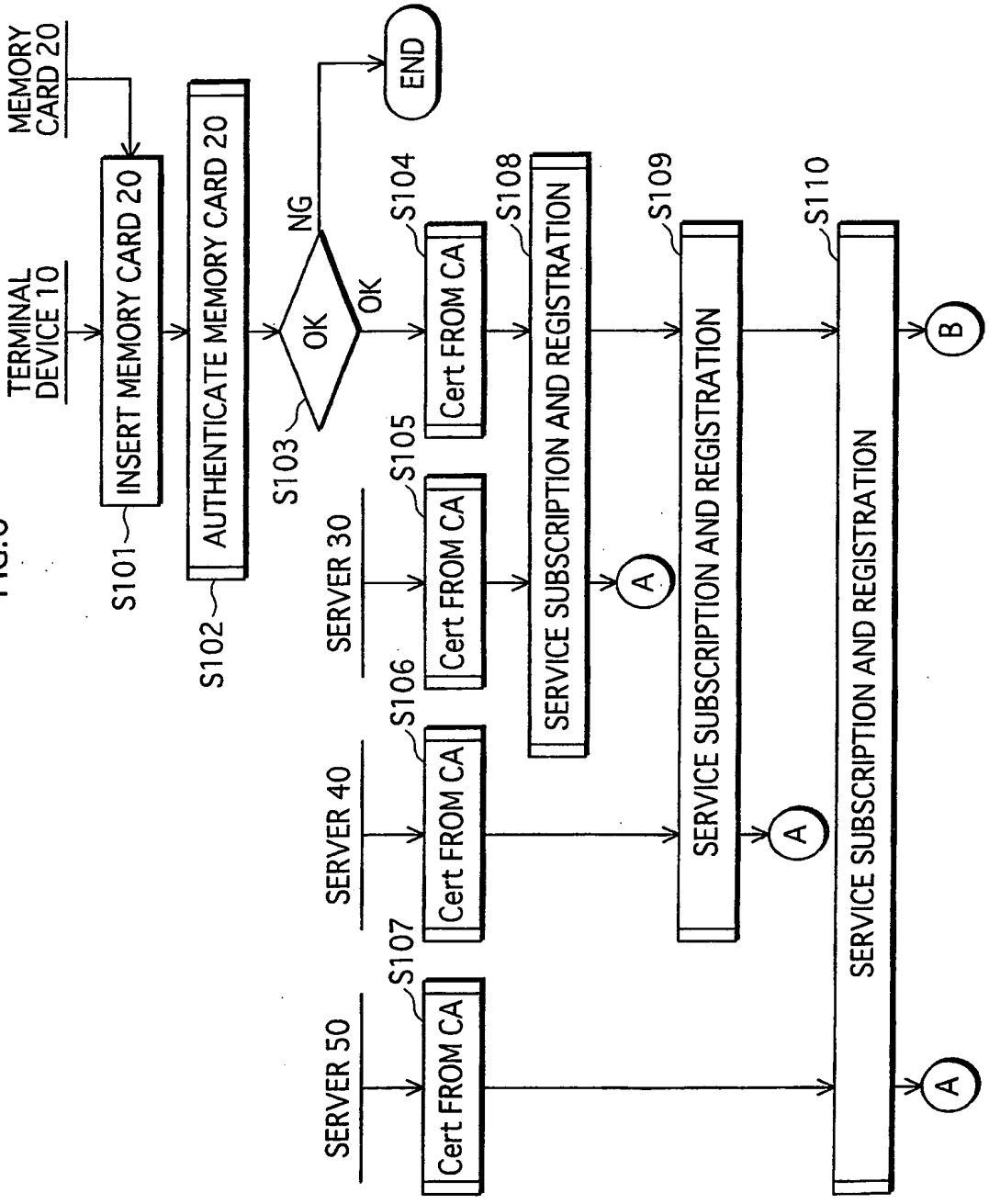

TERMINAL DEVICE 10
MEMORY CARD 20
INSERT MEMORY CARD 20
S101
AUTHENTICATE MEMORY CARD 20
S102
OK
NG
S103
END
OK
SERVER 30
SERVER 40
SERVER 50
S104
Cert FROM CA
S105
Cert FROM CA
S106
Cert FROM CA
S107
Cert FROM CA
S108
SERVICE SUBSCRIPTION AND REGISTRATION
S109
SERVICE SUBSCRIPTION AND REGISTRATION
S110
SERVICE SUBSCRIPTION AND REGISTRATION
A
A
A
A
B

FIG.7

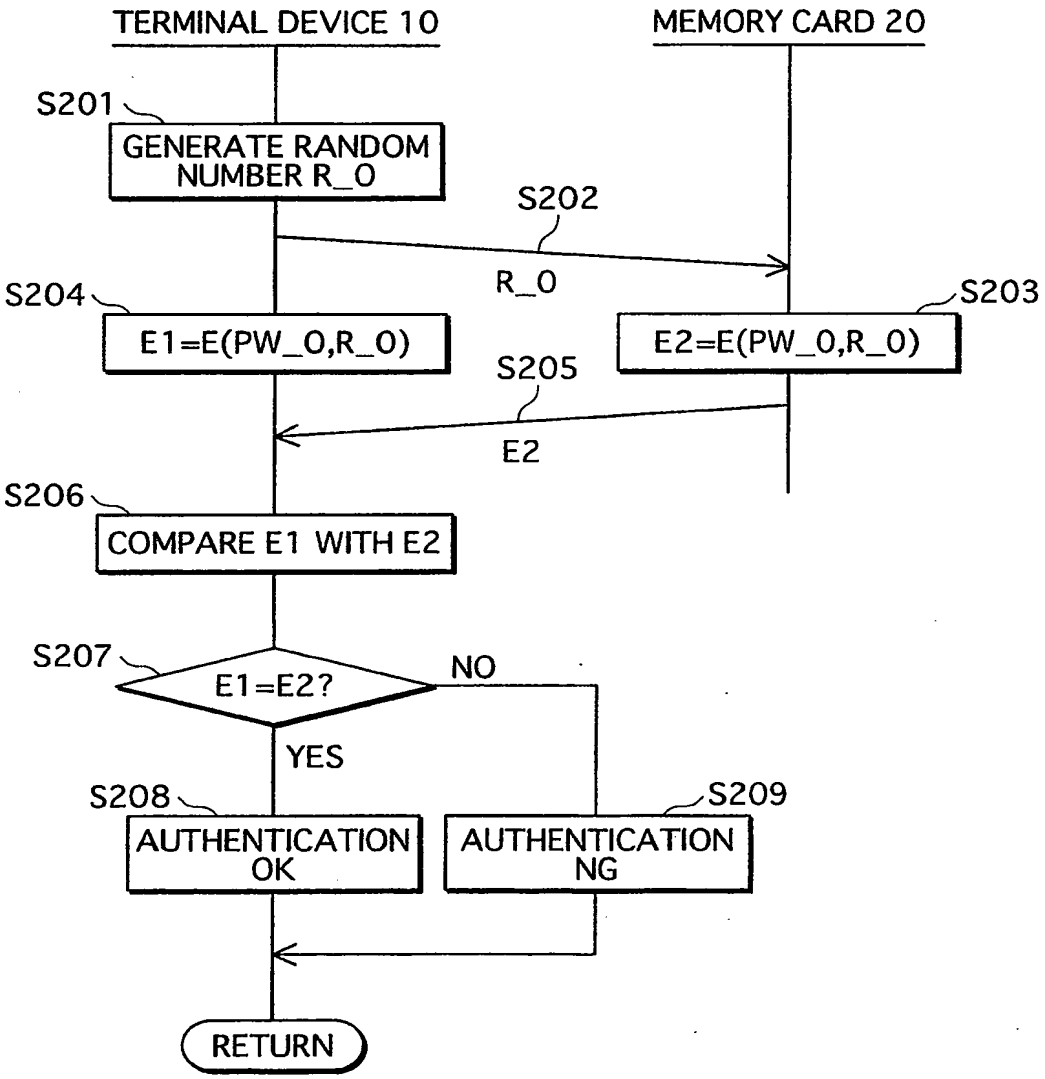

TERMINAL DEVICE 10
MEMORY CARD 20
S201
GENERATE RANDOM NUMBER R_0
S202
R_0
S204
E1=E(PW_0,R_0)
S203
E2=E(PW_0,R_0)
S205
E2
S206
COMPARE E1 WITH E2
S207
E1=E2?
NO
YES
S208
AUTHENTICATION OK
S209
AUTHENTICATION NG
RETURN

FIG.8

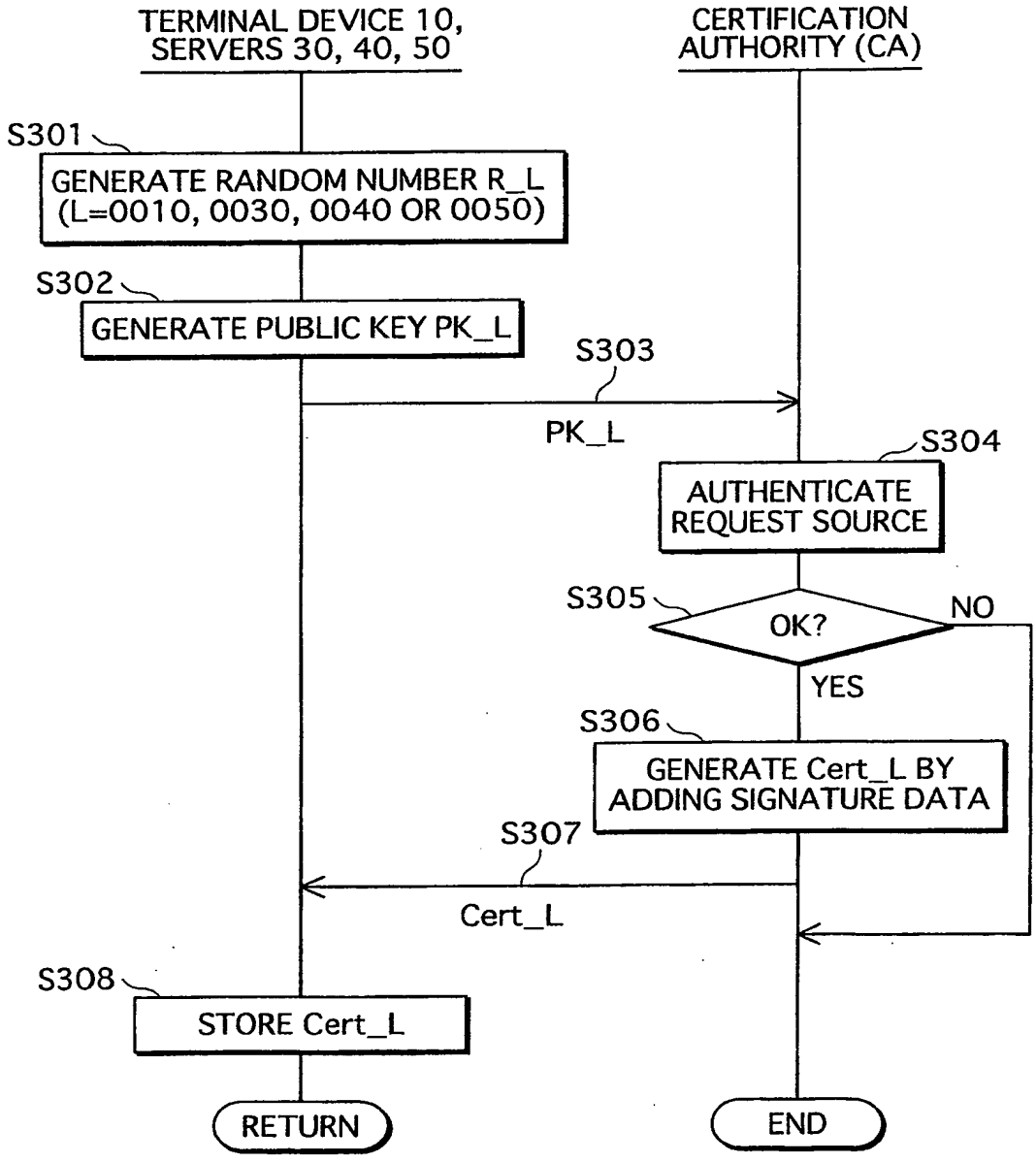

TERMINAL DEVICE 10, SERVERS 30, 40, 50
CERTIFICATION AUTHORITY (CA)
S301
GENERATE RANDOM NUMBER R_L (L=0010, 0030, 0040 OR 0050)
S302
GENERATE PUBLIC KEY PK_L
S303
PK_L
S304
AUTHENTICATE REQUEST SOURCE
S305
OK?
NO
YES
S306
GENERATE Cert_L BY ADDING SIGNATURE DATA
S307
Cert_L
S308
STORE Cert_L
RETURN
END

FIG.9A PUBLIC KEY CERTIFICATION OF TERMINAL DEVICE 10 ISSUED BY CA

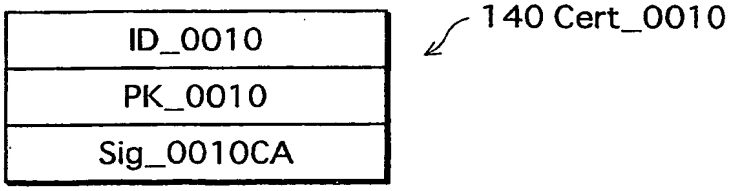


FIG.9B PUBLIC KEY CERTIFICATION OF SERVER 30 ISSUED BY CA

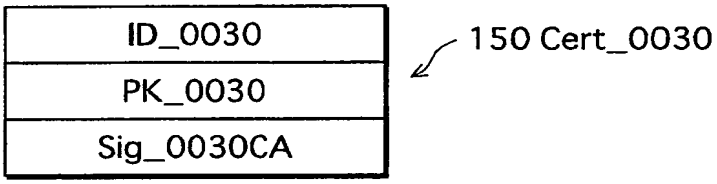


FIG.9C PUBLIC KEY CERTIFICATION OF SERVER 40 ISSUED BY CA

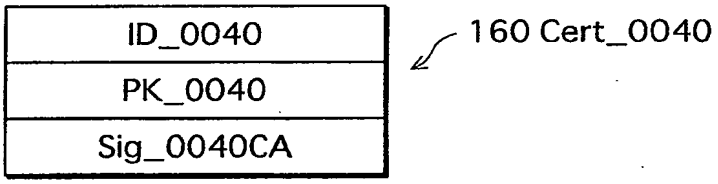


FIG.9D PUBLIC KEY CERTIFICATION OF SERVER 50 ISSUED BY CA

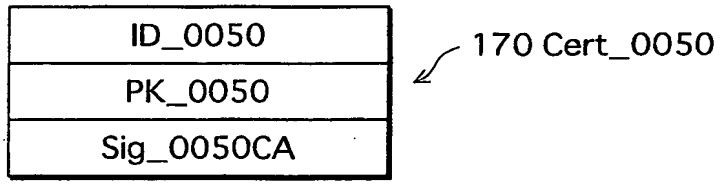


FIG.10

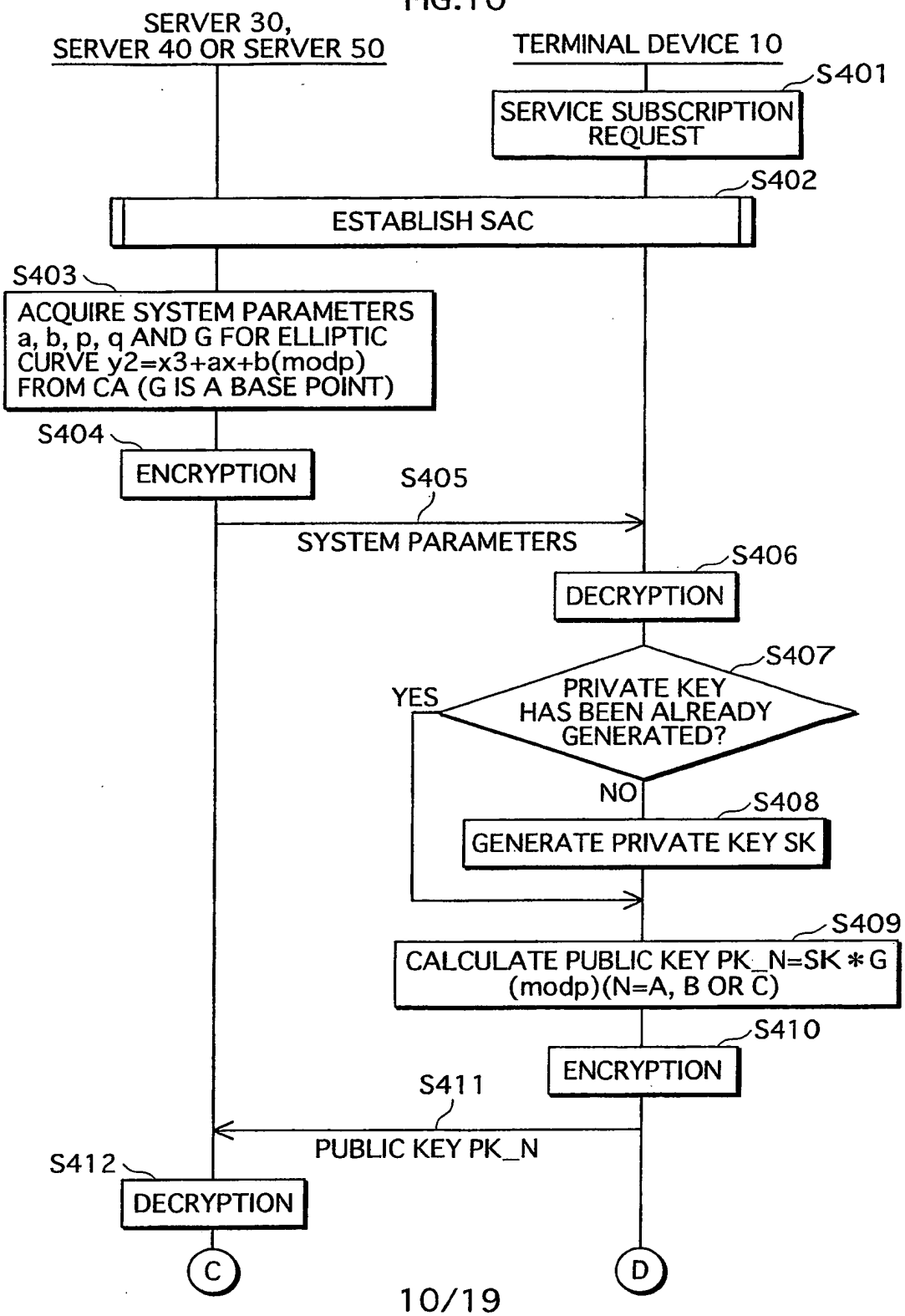

SERVER 30,
SERVER 40 OR SERVER 50
TERMINAL DEVICE 10
S401
SERVICE SUBSCRIPTION REQUEST
S402
ESTABLISH SAC
S403
ACQUIRE SYSTEM PARAMETERS a, b, p, q AND G FOR ELLIPTIC CURVE y2=x3+ax+b(modp) FROM CA (G IS A BASE POINT)
S404
ENCRYPTION
S405
SYSTEM PARAMETERS
S406
DECRYPTION
S407
PRIVATE KEY HAS BEEN ALREADY GENERATED?
YES
NO
S408
GENERATE PRIVATE KEY SK
S409
CALCULATE PUBLIC KEY PK_N=SK*G (modp)(N=A, B OR C)
S410
ENCRYPTION
S411
PUBLIC KEY PK_N
S412
DECRYPTION
C
D

FIG. 11

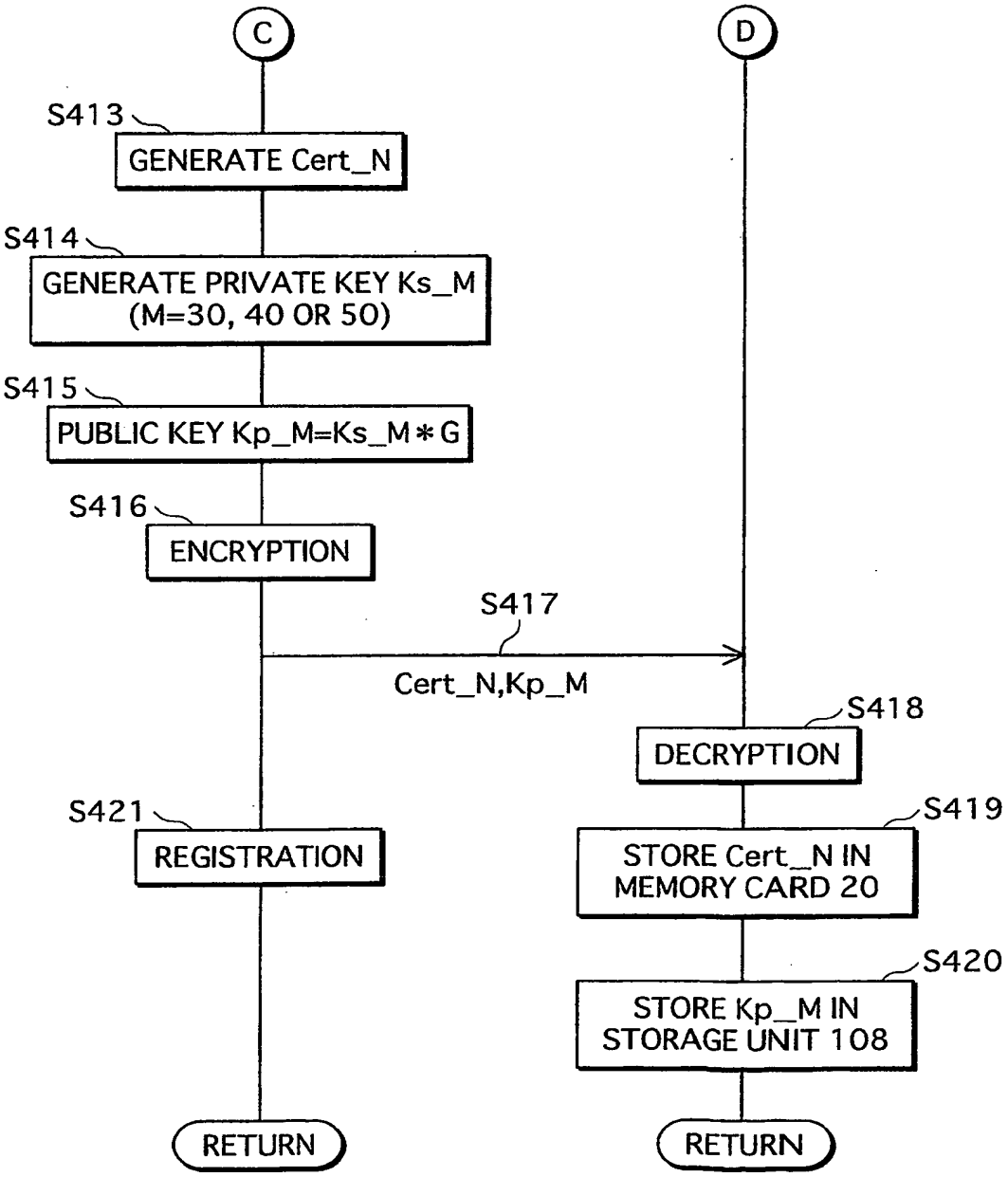

C
D
S413
GENERATE Cert_N
S414
GENERATE PRIVATE KEY Ks_M
(M=30, 40 OR 50)
S415
PUBLIC KEY Kp_M=Ks_M*G
S416
ENCRYPTION
S417
Cert_N,Kp_M
S418
DECRYPTION
S419
STORE Cert_N IN
MEMORY CARD 20
S420
STORE Kp_M IN
STORAGE UNIT 108
S421
REGISTRATION
RETURN
RETURN

FIG.12A PUBLIC KEY CERTIFICATION ISSUED BY SERVER 30

SERVICE ID	SID_0123A
MEMBERSHIP NUMBER	NO_0001
PUBLIC KEY	PK_A
SIGNATURE DATA	Sig_A

210 Cert_A

FIG.12B PUBLIC KEY CERTIFICATION ISSUED BY SERVER 40

SERVICE ID	SID_0321B
MEMBERSHIP NUMBER	NO_0025
PUBLIC KEY	PK_B
SIGNATURE DATA	Sig_B

220 Cert_B

FIG.12C PUBLIC KEY CERTIFICATION ISSUED BY SERVER 50

SERVICE ID	SID_0132C
MEMBERSHIP NUMBER	NO_3215
PUBLIC KEY	PK_C
SIGNATURE DATA	Sig_C

230 Cert_C

FIG.13

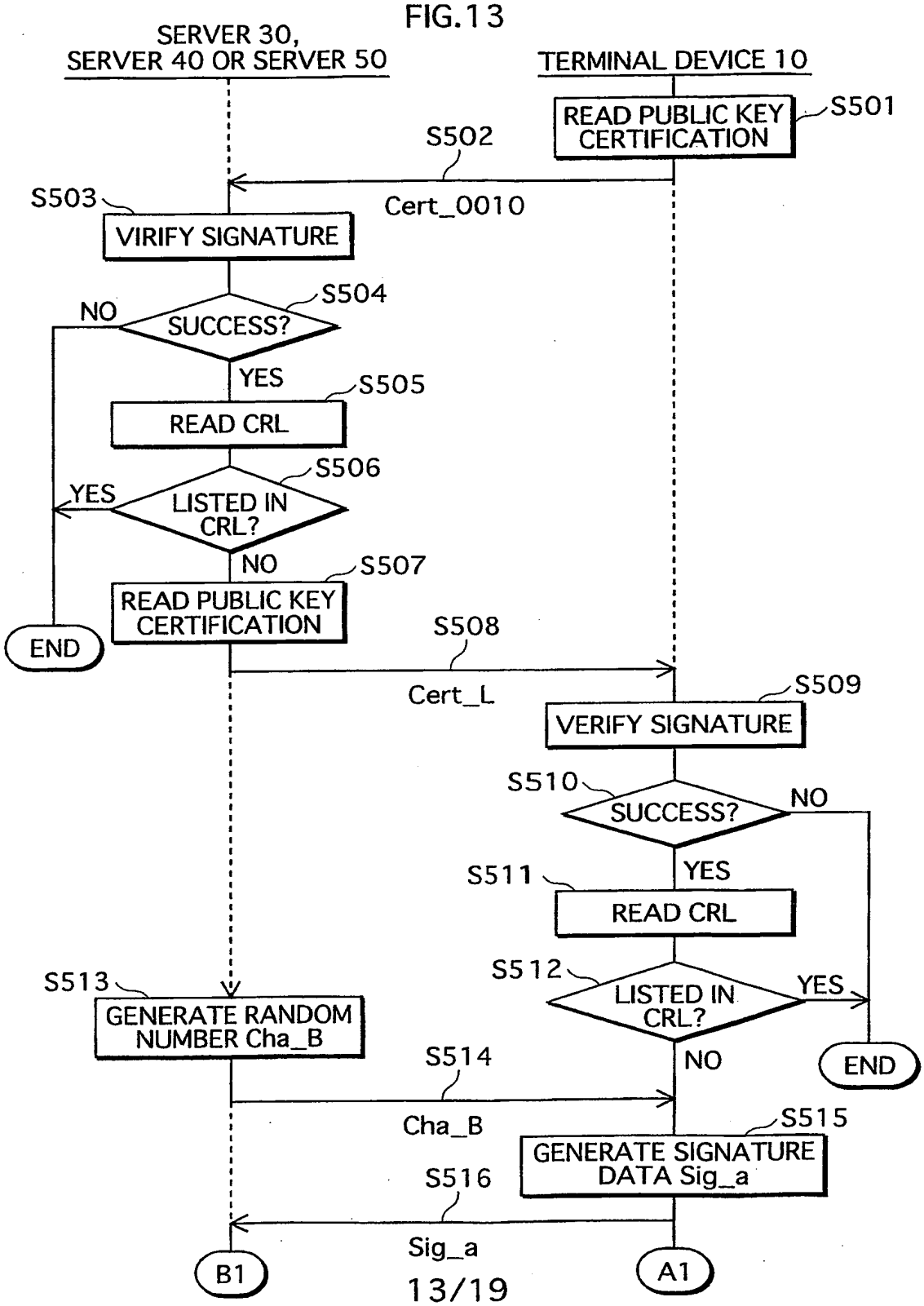

SERVER 30,
SERVER 40 OR SERVER 50
TERMINAL DEVICE 10
READ PUBLIC KEY CERTIFICATION
S501
S502
Cert_0010
S503
VIRIFY SIGNATURE
S504
NO
SUCCESS?
YES
S505
READ CRL
S506
YES
LISTED IN CRL?
NO
S507
READ PUBLIC KEY CERTIFICATION
END
S508
Cert_L
S509
VERIFY SIGNATURE
S510
SUCCESS?
NO
YES
S511
READ CRL
S512
LISTED IN CRL?
YES
NO
END
S513
GENERATE RANDOM NUMBER Cha_B
S514
Cha_B
S515
GENERATE SIGNATURE DATA Sig_a
S516
Sig_a
B1
A1

FIG.14

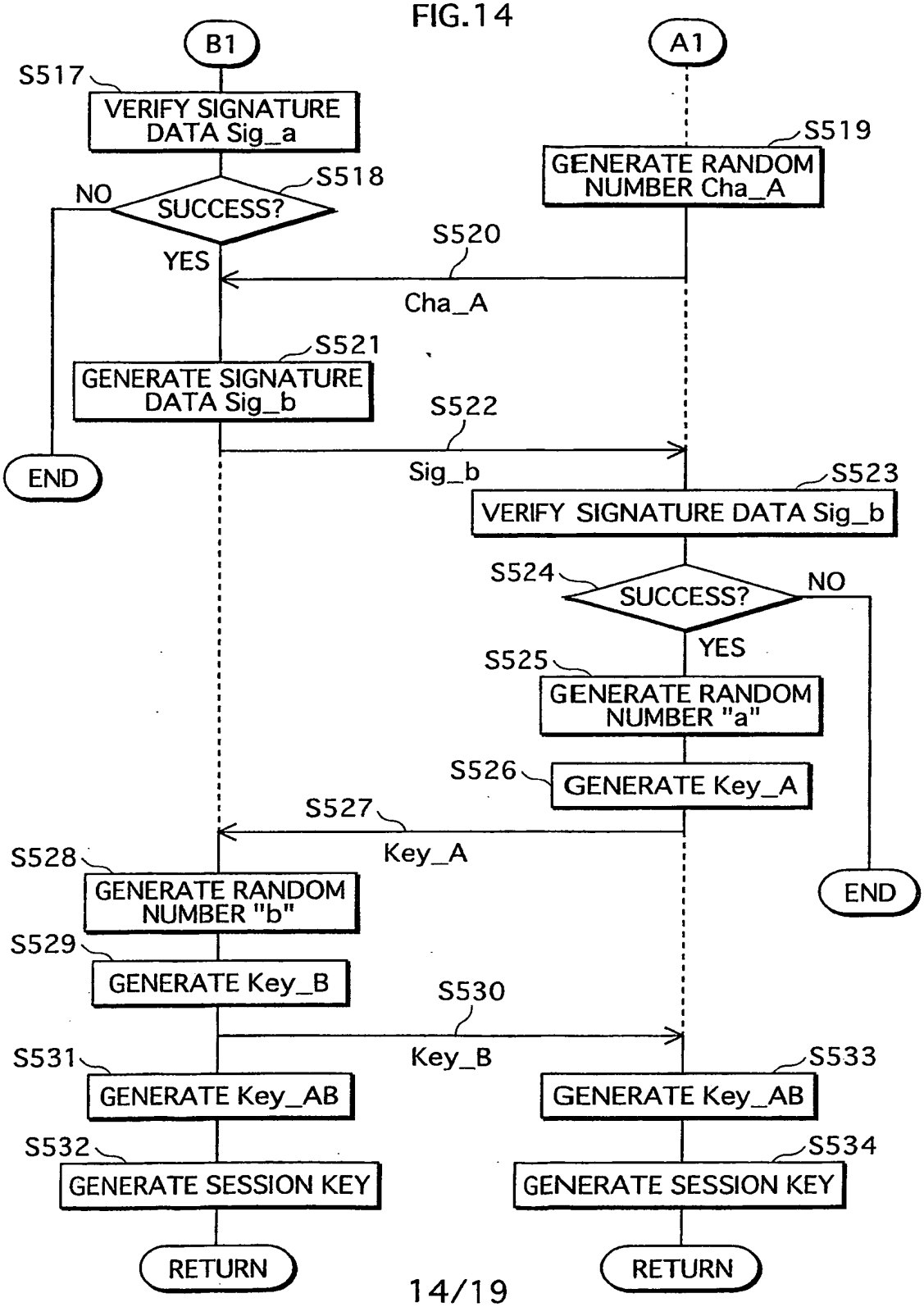

B1
A1
S517
VERIFY SIGNATURE DATA Sig_a
S519
GENERATE RANDOM NUMBER Cha_A
S518
NO
SUCCESS?
S520
YES
Cha_A
S521
GENERATE SIGNATURE DATA Sig_b
S522
END
Sig_b
S523
VERIFY SIGNATURE DATA Sig_b
S524
SUCCESS?
NO
YES
S525
GENERATE RANDOM NUMBER "a"
S526
GENERATE Key_A
S527
Key_A
S528
GENERATE RANDOM NUMBER "b"
END
S529
GENERATE Key_B
S530
Key_B
S531
GENERATE Key_AB
S533
GENERATE Key_AB
S532
GENERATE SESSION KEY
S534
GENERATE SESSION KEY
RETURN
RETURN

FIG.15

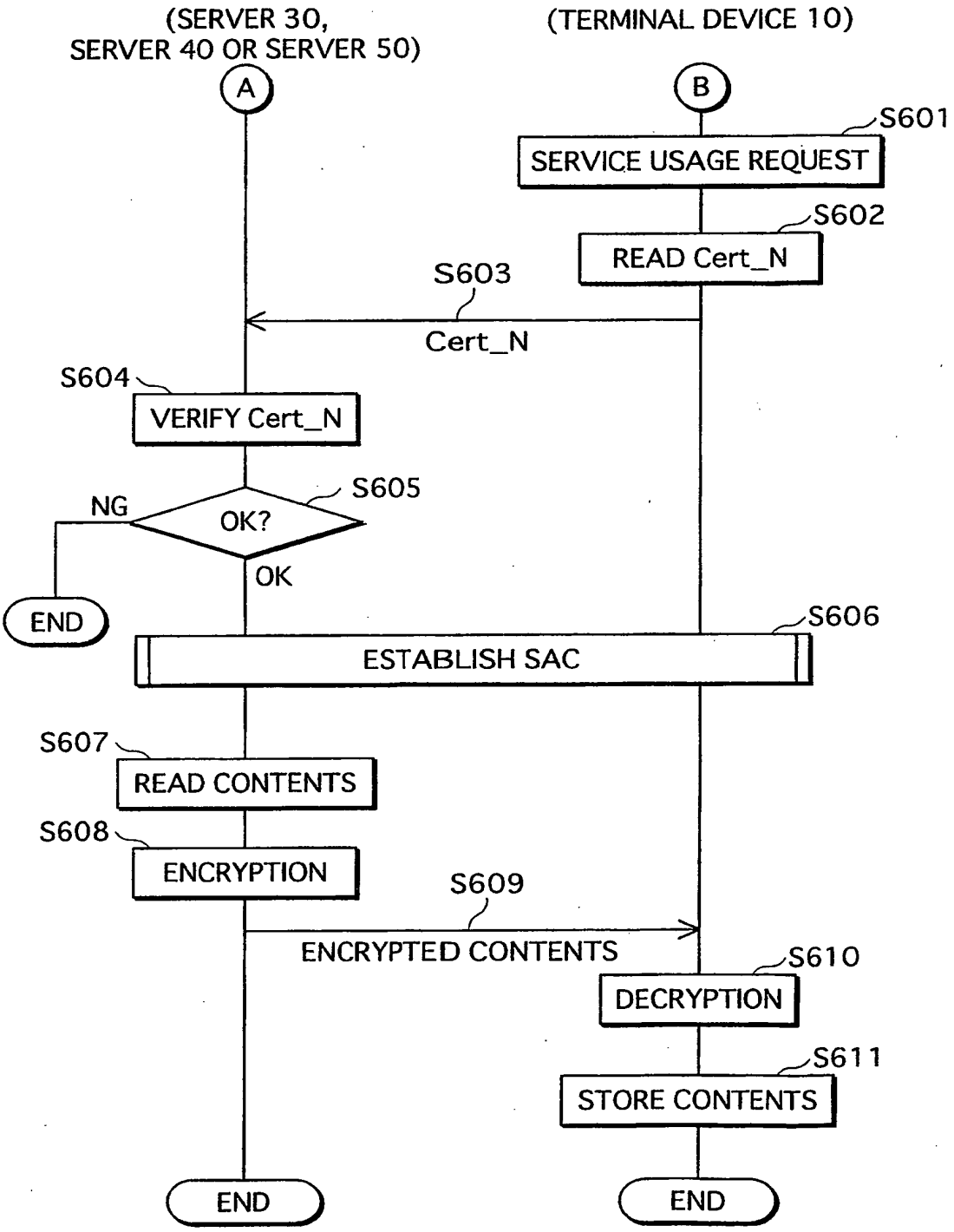

(SERVER 30,
SERVER 40 OR SERVER 50)
(TERMINAL DEVICE 10)
A
B
S601
SERVICE USAGE REQUEST
S602
READ Cert_N
S603
Cert_N
S604
VERIFY Cert_N
S605
NG
OK?
OK
END
S606
ESTABLISH SAC
S607
READ CONTENTS
S608
ENCRYPTION
S609
ENCRYPTED CONTENTS
S610
DECRYPTION
S611
STORE CONTENTS
END
END

FIG.16

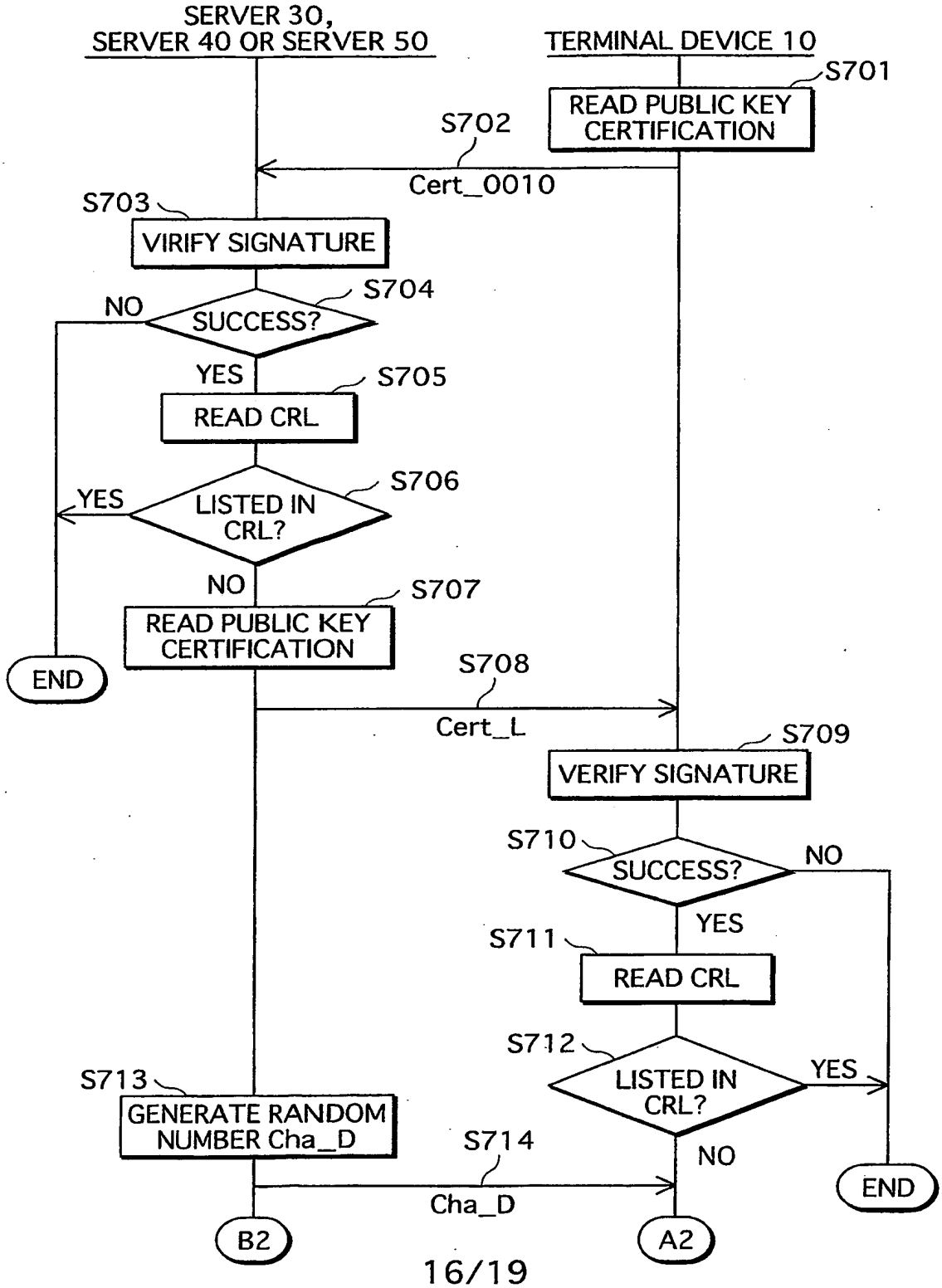

SERVER 30,
SERVER 40 OR SERVER 50
TERMINAL DEVICE 10
S701
READ PUBLIC KEY CERTIFICATION
S702
Cert_0010
S703
VIRIFY SIGNATURE
S704
NO
SUCCESS?
YES
S705
READ CRL
S706
YES
LISTED IN CRL?
NO
S707
READ PUBLIC KEY CERTIFICATION
END
S708
Cert_L
S709
VERIFY SIGNATURE
S710
SUCCESS?
NO
YES
S711
READ CRL
S712
LISTED IN CRL?
YES
S713
GENERATE RANDOM NUMBER Cha_D
S714
NO
Cha_D
END
B2
A2

FIG.17

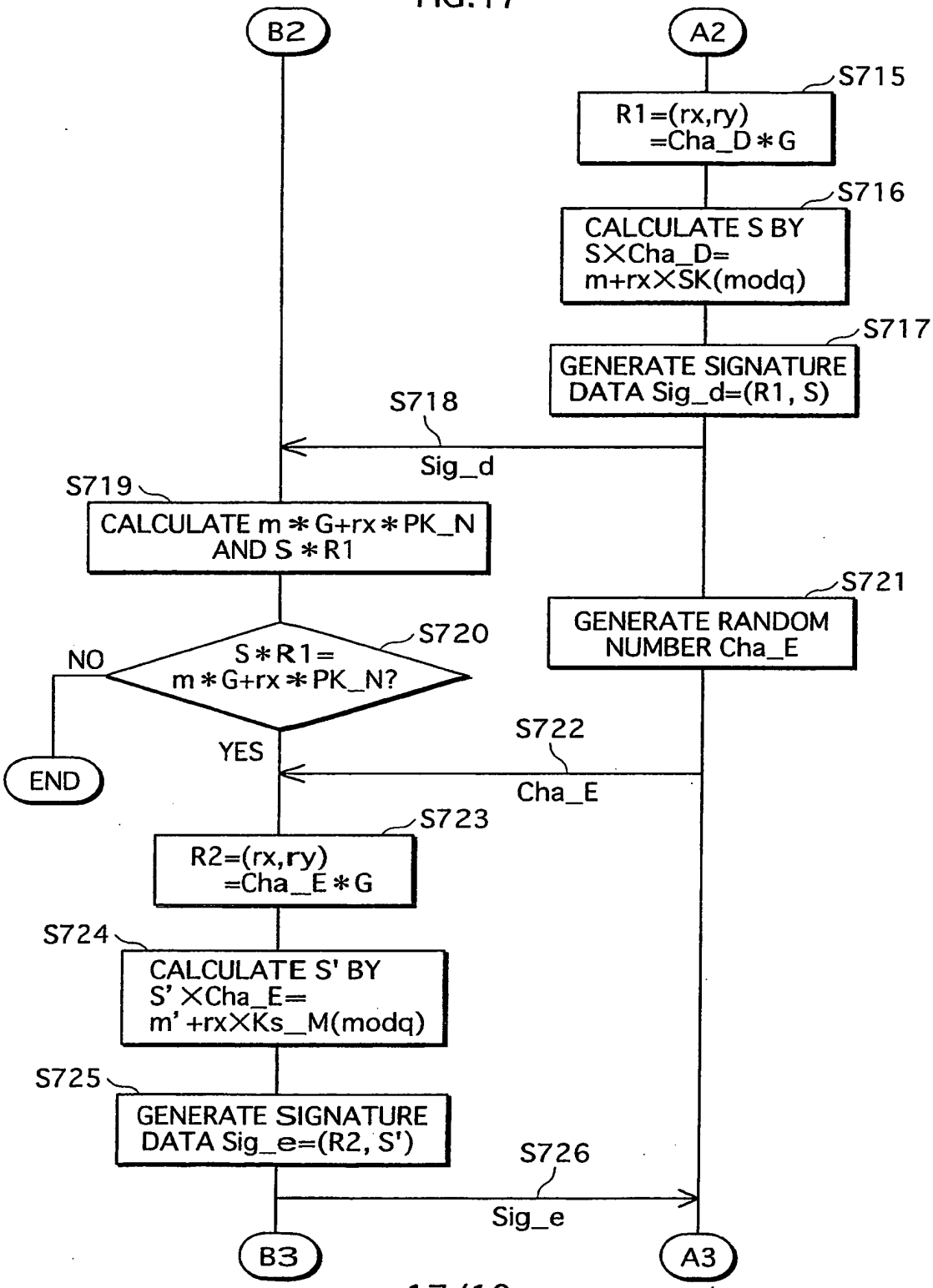

B2
A2
S715
R1=(rx,ry)
=Cha_D*G
S716
CALCULATE S BY
S×Cha_D=
m+rx×SK(modq)
S717
GENERATE SIGNATURE
DATA Sig_d=(R1, S)
S718
Sig_d
S719
CALCULATE m*G+rx*PK_N
AND S*R1
S721
GENERATE RANDOM
NUMBER Cha_E
S720
S*R1=
m*G+rx*PK_N?
NO
YES
END
S722
Cha_E
S723
R2=(rx,ry)
=Cha_E*G
S724
CALCULATE S' BY
S'×Cha_E=
m'+rx×Ks_M(modq)
S725
GENERATE SIGNATURE
DATA Sig_e=(R2, S')
S726
Sig_e
B3
A3

FIG.18

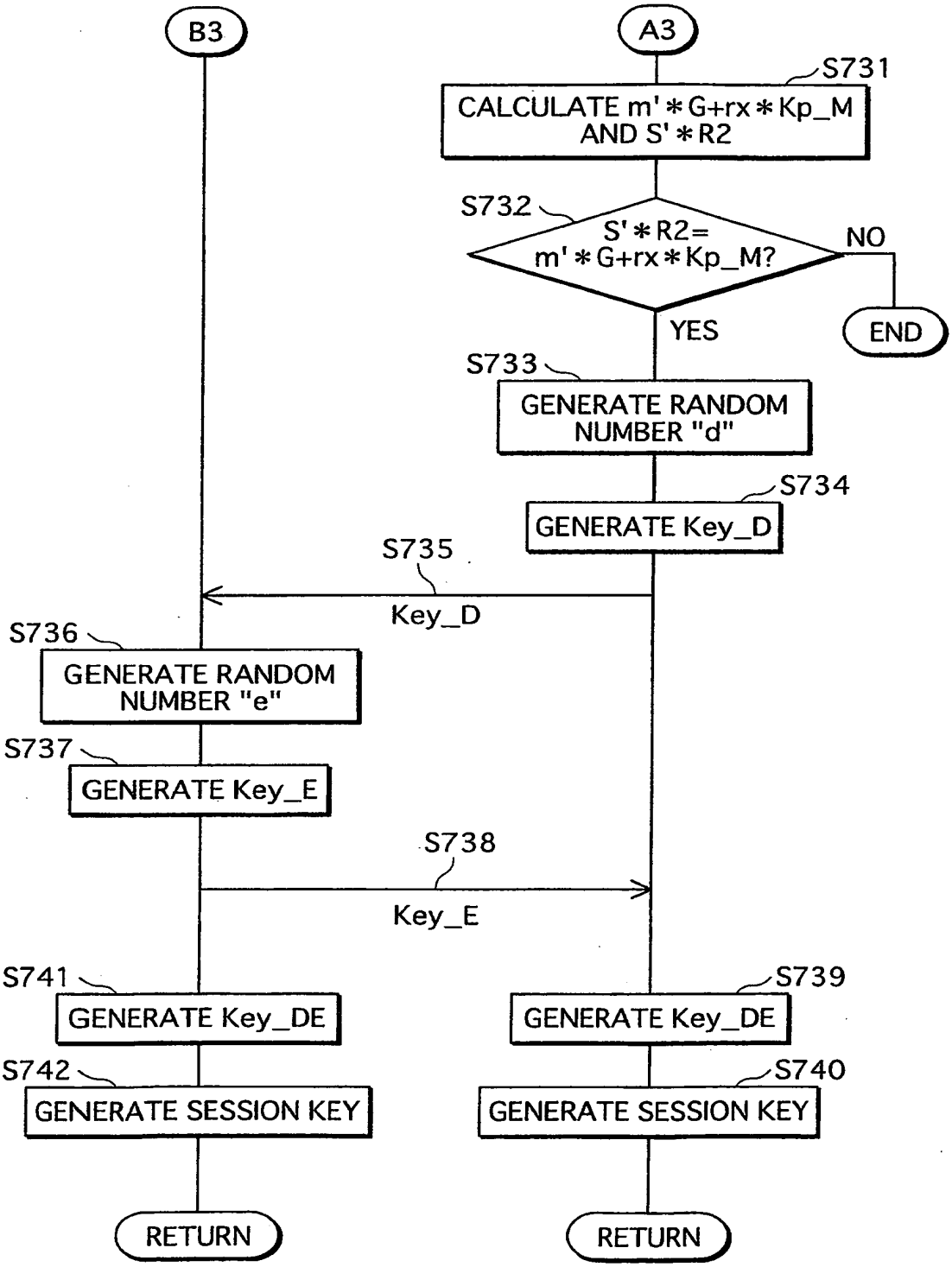
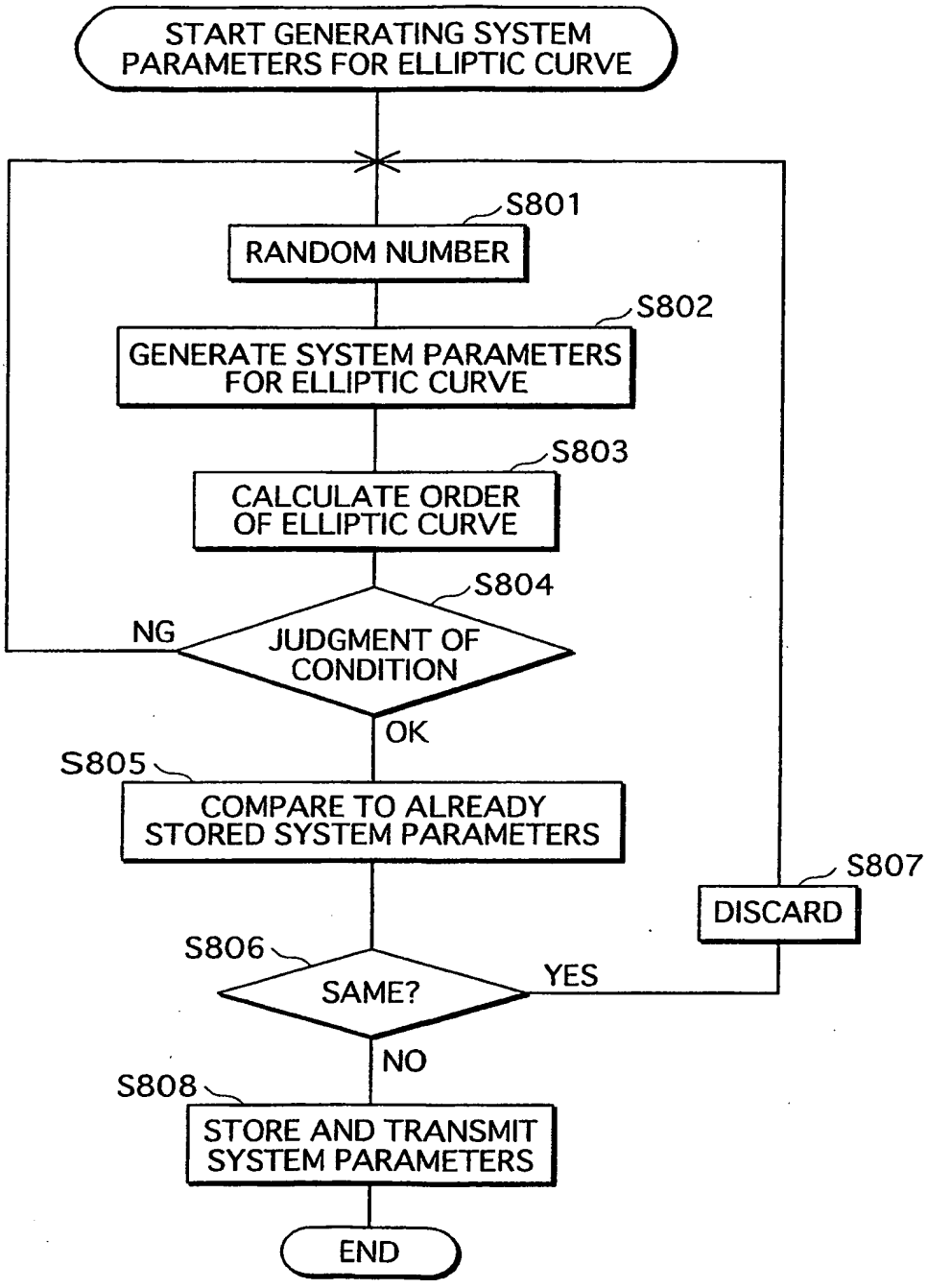

B3
A3
S731
CALCULATE m'*G+rx*Kp_M AND S'*R2
S732
S'*R2= m'*G+rx*Kp_M?
NO
END
YES
S733
GENERATE RANDOM NUMBER "d"
S734
GENERATE Key_D
S735
Key_D
S736
GENERATE RANDOM NUMBER "e"
S737
GENERATE Key_E
S738
Key_E
S741
GENERATE Key_DE
S739
GENERATE Key_DE
S742
GENERATE SESSION KEY
S740
GENERATE SESSION KEY
RETURN
RETURN

FIG.19


START GENERATING SYSTEM PARAMETERS FOR ELLIPTIC CURVE
S801
RANDOM NUMBER
S802
GENERATE SYSTEM PARAMETERS FOR ELLIPTIC CURVE
S803
CALCULATE ORDER OF ELLIPTIC CURVE
S804
JUDGMENT OF CONDITION
NG
OK
S805
COMPARE TO ALREADY STORED SYSTEM PARAMETERS
S806
SAME?
YES
NO
S807
DISCARD
S808
STORE AND TRANSMIT SYSTEM PARAMETERS
END